



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/676,850	09/30/2003	Nicholas M. Ryan	2222.5440000	3054
26111 7590 08/20/2008 STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C. 1100 NEW YORK AVENUE, N.W. WASHINGTON, DC 20005				
EXAMINER				
PALIWAL, YOGESH				
ART UNIT		PAPER NUMBER		
2135				
MAIL DATE		DELIVERY MODE		
08/20/2008		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/676,850

Applicant(s)

RYAN, NICHOLAS M.

Examiner

YOGESH PALIWAL

Art Unit

2135

Period for Reply -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 May 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-22 and 26-31 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-22 and 26-31 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-8508)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

- Applicant's amendment filed on May 28, 2008 has been entered. Applicant has amended claims 1, 6, 14, 16, 26 and 29. Currently claims 1-22 and 26-31 are pending in this application.

Response to Arguments

1. Applicant's arguments regarding claims 1-5 have been fully considered but they are not persuasive for following reasons:
 - Applicant argues that: "Baltzley discloses an encryption server comprising a database. The database of Baltzley may comprise a plurality of encrypted private keys and a plurality of public keys (Baltzley Col.4, Lines 47-50), but the plurality of encrypted private keys and public keys are not stored necessarily as a key pair as "a plurality of cryptographic key pairs, each of the plurality of cryptographic key pairs includes a public key and a private key, " as recited in claim 1 (emphasis added). Thus, even assuming arguendo the database of Baltzley includes the encrypted private keys and public key as pairs, this database includes an encrypted version of the private keys which is not the same as the "key store being configured to store a plurality of cryptographic key pairs, each of the cryptographic key pairs includes a public key and a private key, at least one of the cryptographic key pairs pertaining to a predetermined time" feature of claim 1 (emphasis added)."

- In reply examiner would like to point out at Column 5 lines 2-10 which clearly recites that the private keys and public keys are stored as a key pair (see, Column 5, lines 2-10, "The New User computer program 215 then encrypts the private key and transmits the encrypted private key 320 and public key 325 back to the encryption server 105. The Server computer program 335 directs the encryption server 105 to receive the encrypted private key 320 and the public key 325 from the client machine 110 and store them in the encryption server 105 database 315." and also see Fig. 3, Numeral 320 and 325). Therefore, Baltzley clearly discloses the limitation of "a plurality of cryptographic key pairs, each of the plurality of cryptographic key pairs includes a public key and a private key" as required by claim 1. Furthermore, applicants argument regarding storing an encrypted version of private key is also not found persuasive because there is nothing in claim 1 that restrict private keys from being encrypted.
- Applicant further argues that, "Second, Applicant maintains that the combination of Baltzley and Batten-Carew does not teach or suggest "wherein a data portion of the secured electronic file was previously secured using a document key, and wherein the document key was previously secured by the public key of the at least one of the cryptographic key pairs pertaining to the predetermined time," as recited in claim 1, as amended."
- Inclusion of new limitations in claim 1 has triggered new grounds of rejection and new reference teaches these limitations.

2. Applicant's arguments with respect to claims 6-9 and 26-29 have been considered but are moot in view of the new ground(s) of rejection.
3. Applicant's arguments, see pages 16-18, filed on May 25, 2008, with respect to the rejection(s) of claim(s) 10, 11, 12, 13-15 and 30 under U.S.C. 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of En-Seung and Batten-Carew.
4. Applicant's arguments, see pages 19-21, filed on May 25, 2008, with respect to the rejection(s) of claim(s) 16-22 and 31 under U.S.C. 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of En-Seung and Batten-Carew.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baltzley (US 6,292,895 B1), hereinafter "Baltzley" in view of Angelo et al. (US

5,923,754), hereinafter, "Angelo" and further in view of Batten-Carew et al. (US 6,603,857 B1), hereinafter "Batten-Carew".

Regarding **Claim 1**, Baltzley discloses a file security system for restricting access to electronic files, said file security system comprising:

a key store being configured to store a plurality of cryptographic key pairs, each of the plurality of cryptographic key pairs includes a public key and a private key (see, Fig. 2, Numerals 320, and 325).

an access manager (see Fig. 3, Numeral 220) operatively connected to said key store, said access manager being configured to determine whether the private key of the at least one of the cryptographic key pairs is permitted to be provided to a requester (see Column 2, lines 41-52 and also Column 5 lines 2-10).

wherein the requester requires the private key of the at least one of the cryptographic key pair to access a secured electronic file (see Column 2, lines 51-52), and wherein the secured electronic file was previously secured using the public key of the at least one of the cryptographic key pairs (See Column 2, lines 55-56).

Baltzley directly encrypt the electronic file using the public key and therefore does not teach that a data portion of the secured electronic file was previously secured using a document key and wherein the document key was previously secured by the public key of the cryptographic key pair.

However, hybrid encryption was well-known at the time invention was made. Angelo discloses encrypting the message using a document key and the encrypting the document key using a public key (see, Column 3, lines 13-22).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use, instead of public key directly encrypting the documents in the system of Baltzley, the technique of hybrid encryption as taught by Angelo because encrypting the message with the symmetric algorithm is faster than asymmetric algorithm and using public key just to encrypt the document key reduces the chances for plaintext attacks. In other words, hybrid encryption provides the security of public-key encryption at the same time processing messages faster than asymmetric encryption by using symmetric key for data encryption.

Baltzley does not disclose a cryptographic key that pertains to a predetermined time.

Batten-Carew discloses a method and apparatus for controlling release of time-sensitive information is accomplished by a server that establishes access information for a specific future time as passed (abstract). The method includes at least one of the cryptographic key pairs pertaining to a predetermined time (column 3 lines 40-47); key pairs pertaining to the predetermined time is permitted to be provided to a requester based on a current time (Fig. 3), wherein the requester requires the private key of the at least one of the cryptographic key pairs pertaining to the predetermined time to access a secured electronic file (column 3 lines 48-55), and wherein the secured electronic file was previously secured using the public key of the at least one of the cryptographic key pairs pertaining to the predetermined time (Fig. 1).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the time-based key of Batten-Carew in the system of

Baltzley. One of ordinary skill in the art would have been motivated to do this because the method of Batten- Carew would allow time-sensitive information to be released at any time and accessed only at a specific future time based on the release of access information relating to the specific future time (column 2 lines 29-33).

Regarding **Claim 2**, the rejection of claim 1 is incorporated and Baltzley does not teach an access manager only provides the private key of the at least one of the cryptographic key pairs pertaining to the predetermined time to the requester if the predetermined time is greater than or equal to the current time.

Batten-Carew discloses a system, wherein said access manager only provides the private key of the at least one of the cryptographic key pairs pertaining to the predetermined time to the requester if the predetermined time is greater than or equal to the Current time (Fig. 3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the time-based key of Batten-Carew in the system of Baltzley. One of ordinary skill in the art would have been motivated to do this because the method of Batten- Carew would allow time-sensitive information to be released at any time and accessed only at a specific future time based on the release of access information relating to the specific future time (column 2 lines 29-33).

Regarding **Claim 3**, the rejection of claim 1 is incorporated and Baltzley further discloses wherein the requester is a client module that operatively connects to said access manager over a network (see Figs. 3 and 4).

Regarding **Claim 4**, the rejection of claim 1 is incorporated and Baltzley does not disclose a system wherein said document security system further comprises: at least one client module, said client module assists a user in selecting the predetermined time, and said client module secures the electronic file using the public key of the at least one of the cryptographic key pairs pertaining to the predetermined time so as to provide a time-based access restriction to the electronic file.

Batten-Carew discloses a system wherein said document security system further comprises: at least one client module, said client module assists a user in selecting the predetermined time, and said client module secures the electronic file using the public key of the at least one of the cryptographic key pairs pertaining to the predetermined time so as to provide a time-based access restriction to the electronic file (Fig. 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the time-based key of Batten-Carew in the system of Baltzley. One of ordinary skill in the art would have been motivated to do this because the method of Batten-Carew would allow time-sensitive information to be released at any time and accessed only at a specific future time based on the release of access information relating to the specific future time (column 2 lines 29-33).

Regarding **Claim 5**, the rejection of claim 4 is incorporated and Baltzley does not disclose wherein said client module further assists in unsecuring the secured electronic file by acquiring the private key of the at least one of the cryptographic key pairs that pertaining to the predetermined time from said key store, and then unsecuring the

secured electronic file using the private key of the at least one of the cryptographic key pairs that pertaining to the predetermined time

Batten-Carew discloses a system wherein said client module further assists in unsecuring the secured electronic file by acquiring the private key of the at least one of the cryptographic key pairs that pertaining to the predetermined time from said key store, and then unsecuring the secured electronic file using the private key of the at least one of the cryptographic key pairs that pertaining to the predetermined time (Fig. 3 and Fig. 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the time-based key of Batten-Carew in the system of Baltzley. One of ordinary skill in the art would have been motivated to do this because the method of Batten- Carew would allow time-sensitive information to be released at any time and accessed only at a specific future time based on the release of access information relating to the specific future time (column 2 lines 29-33).

Claims 6-9 and 26-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over En-Seung et al.(US 6,892,306 B1), hereinafter, "En-Seung") in view of Batten-Carew and further in view of Singhal et al. (US 6,851,050 B2), hereinafter "Singhal").

Regarding **Claims 6, 26 and 29**, En-Seung discloses an apparatus, a corresponding method and a corresponding computer program for controlling release of time-sensitive information, said method comprising:

Identifying an electronic document to be secured, the electronic document having at least a data portion that contains data (see, Column 5, lines 57-61);

generating a access key (see Column 9, lines 9-11);

securing the electronic document through use of the access key and a document key to produce a secured electronic document (see Column 3, lines 14-22 and see Figs. 10 and also Column 5, lines 6-8); and

storing the secured electronic document (see Column 6, lines 54-59).

En-Seung discloses user key that encrypt document key and document key that encrypts the contents. However, En-Seung does not explicitly disclose that the user key is a time-based access key.

Batten-Carew discloses a method and apparatus for controlling release of time-sensitive information is accomplished by a server that establishes access information for a specific future time as passed (abstract). Batten-Carew discloses using time-based access key for the predetermined time (Column 3, lines 34-40).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the time-based key of Batten-Carew in the system of En-Seung. One of ordinary skill in the art would have been motivated to do this because the method of Batten- Carew would allow time-sensitive information to be released at any time and accessed only at a specific future time based on the release of access information relating to the specific future time (column 2 lines 29-33).

Even though the combination of En-Seung and Batten-Carew discloses generating time-based access key for a predetermined time it does not explicitly

discloses a step of determining whether a time-based access key is already available for a predetermined time, otherwise generating a time-based access key for the predetermined time. Batten-Carew is just missing the step of checking to see if the time-based access key is already generated and only generate new time-based access key if one does not exist.

Singhal discloses a condition where prior to generating a key, system check to see the key is already generated and only generates a new key if one does not exist (see Column 18, lines 30-60).

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to generate, the time-based access key of the combined system of En-Seung and Batten-Carew, only if the key doesn't already exist. One of ordinary skill in the art would have been motivated to check this condition prior to generating new time-based access key in a case where sender is sending more than one document and all document are suppose to release on the same time. In such a condition it would be appropriate to simply use the same time-based access key rather than generating multiple time-based access keys for the same predetermined time.

Regarding **Claims 7 and 27**, Batten-Carew discloses a method wherein the time-based access key has an access time associated therewith (column 3 lines 4-23').

Regarding **Claims 8 and 28**, Batten-Carew discloses a method wherein said method further comprises: storing the time-based access key at a remote key store, and wherein the time-based access key is subsequently retrievable from the remote key

store only if the current time equals or exceeds the access time associated with the time-based access key (Fig. 1 and Fig. 3).

Regarding **Claim 9**, Batten-Carew discloses a method wherein said method is performed on a client machine that operatively receives the time-based access key from the remote key store over a network (Fig. 1 and column 3 lines 32-35).

Claims 10-22 and 30-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over En-Seung in view of Batten-Carew.

Regarding **Claims 10 and 30**, En-Seung et al. (US 6,892,306 B1) discloses a method and a corresponding computer program for restricting access to an electronic document, said method comprising:

Identifying an electronic document (digital information) to be secured, the electronic document to be secured, the electronic document having at least a data portion that contains data (Column 5, lines 57-61);

obtaining a document key (See Column 3, lines 25-28, "temporary validation key");

encrypting the data portion of the electronic document using the document key to produce an encrypted data portion (see Column 3, lines 25-28);

obtaining a access key (See Column 3, lines 14-22, user key);

encrypting the document key using the access key to produce an encrypted document key (see Column 3, lines 14-22, temporary validation key is encrypted using user key);

forming a secured electronic document from at least the encrypted data portion and the encrypted document key (see Figs. 10 and also Column 5, lines 6-8).

storing the secured electronic document (see Column 6, lines 54-59)

En-Seung discloses user key that encrypt document key and document key that encrypts the contents. However, En-Seung does not explicitly discloses that the user key is a time-based access key.

Batten-Carew discloses a method and apparatus for controlling release of time-sensitive information is accomplished by a server that establishes access information for a specific future time as passed (abstract). Batten-Carew discloses using time-based access key (Column 3, lines 34-40).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the time-based key of Batten-Carew in the system of En-Seung. One of ordinary skill in the art would have been motivated to do this because the method of Batten- Carew would allow time-sensitive information to be released at any time and accessed only at a specific future time based on the release of access information relating to the specific future time (column 2 lines 29-33).

Regarding **Claim 11**, the combination of En-Seung and Batten-Carew further discloses wherein the time-based access key is a public time-based access key (see Batten-Carew, Column 3, lines 48-64)

Regarding **Claim 12**, the combination of En-Seung and Batten-Carew further discloses wherein the time-based access key has an access time associated therewith (see Batten-Carew, column 3 lines 4-23 and Fig. 2)

Regarding **Claim 13**, the combination of En-Seung and Batten-Carew further discloses wherein the time-based access key is available from a remote key store when the current time is equal to or greater than the access time associated with the time-based access key (see Batten-Carew, Fig. 3).

Regarding **Claim 14**, the combination of En-Seung and Batten-Carew further discloses wherein the access time is a day of a year and the time-based access keys are unique for each day of the year (see Batten-Carew, Fig. 2).

Regarding **Claim 15**, the combination of En-Seung and Batten-Carew further discloses further discloses wherein said method is performed on a client machine that operatively receives the time-based access key from the remote key store over a network (see Batten-Carew, Fig. 1 and Column 3 lines 32-35).

Claims 16-22 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over En-Seung in view of Batten-Carew.

Regarding **Claims 16 and 31**, En-Seung discloses a method and a corresponding computer program for accessing a secured electronic document by a requester, the secured electronic document having at least a header portion and an encrypted data portion (see, Fig. 10), said method comprising:

obtaining an access key (See Fig. 21A, Numeral S430, and also Column 3, lines 14-22, user key);

obtaining an encrypted document key from the header portion of the secured electronic document (see, Column 15, lines 35-51);

decrypting the encrypted document key using the access key produce a document key (see, Column 15, lines 63-67);

decrypting an encrypted data portion of the secured electronic document using the document key to produce a data portion (see, Column 16, lines 10-14); and supplying the data portion to the requester (see, Fig. 21B, Numeral S470).

Peterson discloses obtaining an encrypted document key however he does not explicitly discloses obtaining an encrypted document key from the header portion of the secured electronic document.

En-Seung discloses user key that encrypt document key and document key that encrypts the contents. However, En-Seung does not explicitly disclose that the user key is a time-based access key.

Batten-Carew discloses a method and apparatus for controlling release of time-sensitive information is accomplished by a server that establishes access information for a specific future time as passed (abstract). Batten-Carew discloses using time-based access key (Column 3, lines 34-40).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the time-based key of Batten-Carew in the system of En-Seung. One of ordinary skill in the art would have been motivated to do this because the method of Batten- Carew would allow time-sensitive information to be released at any time and accessed only at a specific future time based on the release of access information relating to the specific future time (column 2 lines 29-33).

Regarding **Claim 17**, the combination of En-Seung and Batten-Carew further discloses wherein the time-based access key is identified by an indicator within a header portion of the secured electronic document (see, En-Seung Column 15, lines 35-51 as modified by Batten-Carew).

Regarding **Claim 18**, the combination of En-Seung and Batten-Carew further discloses using a private time-based access key (see Batten-Carew, Column 3, lines 48-64).

Regarding **Claim 19**, Peterson discloses wherein the time-based access key being obtained is acquired from a server (see Batten-Carew, Fig. 1 and Column 3 lines 32-35).

Regarding **Claim 20**, the combination of En-Seung and Batten-Carew further discloses wherein said obtaining of the time-based access key is dependent on the current time (see Batten-Carew, column 3 lines 4-23 and Fig. 2).

Regarding **Claim 21**, the combination of En-Seung and Batten-Carew further discloses wherein the time-based access key is associated with an access time, and wherein said obtaining of the time-based access key is permitted when the current time is greater than or equal to the access time (see Batten-Carew, Fig. 3).

Regarding **Claim 22**, the combination of En-Seung and Batten-Carew further discloses wherein, if permitted, during said obtaining step the time-based access key is obtained from a server (see Batten-Carew, Fig. 1 and Column 3 lines 32-35).

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to YOGESH PALIWAL whose telephone number is (571)270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Y. P./
Examiner, Art Unit 2135
/KimYen Vu/
Supervisory Patent Examiner, Art Unit 2135